**REMARKS**

Claims 1-33 are currently pending in the subject application and are presently under consideration. Favorable reconsideration of the subject patent application is respectfully requested in view of the comments herein.

I.      **Rejection of Claims 1-7, 9-19, and 29-33 Under 35 U.S.C. §102(b)**

Claims 1-7, 9-19, and 29-33 stand rejected under 35 U.S.C. §102(b) as being anticipated by Abraham, *et al.* (US 5,539,906). Examiner did not indicate that claims 30-33 were officially rejected under this section, but applicants' representative assumes that Examiner has rejected these claims as he has offered no reason for rejection for these claims under this section of the subject Office Action. Nevertheless, it is requested that this rejection be withdrawn for at least the following reason. Abraham, *et al.* fails to teach or suggest each and every element recited in the subject claims.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "***each and every element*** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)) (emphasis added).

The subject matter claimed herein relates to a system that automates security in an industrial control environment by automatically creating security profiles for industrial automation devices in the environment and enforcing these profiles with respect to accessing entities. Such profiles may define different levels of access for various entities. To this end, independent claim 1 (and similarly independent claim 29) recites *an asset component that **defines an industrial automation device;** an access component that **defines a security attribute associated with the industrial automation device;** and a security component that **regulates access to the industrial automation device** based upon the security attribute.* Abraham, *et al.* fails to teach or suggest such claimed aspects.

Abraham, *et al.* generally relates to a system for regulating data security in a data processing system. In particular, data stored in the data processing system is used by an

industrial process in manufacturing an object. Before the industrial process uses the data, however, the data is accessed and modified by a number of individuals as the object being manufactured moves through the design and ultimately to the manufacturing stage. Specifically, engineering change control is discussed in Abraham, *et al.* whereby design data for the object being manufactured moves through various phases and at each phase, only the groups meant to further the design at that step in the process, have access to the data. (*See* col. 9, line 63 – col. 10, line 14). However, Abraham, *et al.* fails to disclose or suggest ***defining an industrial automation device, defining a security attribute associated with the industrial automation device***, and ***regulating access to the industrial automation device***.

First and foremost, the system disclosed in Abraham, *et al.* is not regulating access to an industrial automation device as described in the subject claims; rather, the system in Abraham, *et al.* is regulating access to data that will eventually be used in conjunction with an industrial process that will control manufacture of a desired object. This is evident in the very nature of the system disclosed in Abraham, *et al.* – the data is controlled through the design process and then access to the data is closed before the device is manufactured at disparate manufacturing plants. (*See* col. 6, lines 31-44, particularly, the manufacturing engineers approve the manufacturing change as ready to be implemented on the shop floor, and then the data is closed such that no more changes may be made by anyone *to the data*). Thus, Abraham, *et al.* is regulating access merely to data in a data processing system and not the industrial device directly. Contrarily, applicants' claimed subject matter is regulating access to the industrial automation devices themselves.

Moreover, the system described in Abraham, *et al.* does not define an industrial automation device, nor does it define a security attribute associated with such a device as recited in the subject claims. Abraham, *et al.* merely regulates access to the design data related to an object to be manufactured, and thus, does not disclose the foregoing aspects either. The fact that the data being regulated may be accessed by an industrial process at some time in the future is of no consequence. Thus, Abraham, *et al.* still fails to teach or suggest regulating access and generally defining security profiles and attributes for industrial automation devices. Since Abraham, *et al.* fails to teach or suggest each and

every element recited in claims 1 and 29, rejection of these claims, as well as claims 2-7, 9-19 and 30-33 which depend therefrom, should be withdrawn.


**II.      Rejection of Claims 20-28 Under 35 U.S.C. §103(a)**

Claims 20-28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Flowers, *et al.* (US 6,957,348) in view of Abraham, *et al.*  It is requested that this rejection be withdrawn for at least the following reasons.  Flowers, *et al.* and Abraham, *et al.*, whether taken alone or in combination, fail to disclose, teach, or suggest every element in the subject claims.

> To reject claims in an application under §103, an examiner must establish a *prima facie* case of obviousness.  A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there **must be some suggestion or motivation**, either in the references themselves or in the knowledge generally available to **one of ordinary skill in the art, to modify the reference or to combine reference teachings**.  Second there must be a **reasonable expectation of success**.  Finally, the prior art reference (or references when combined) **must teach or suggest all the claim limitations**.  *See* MPEP §706.02(j).  The **teaching or suggestion to make the claimed combination** and the reasonable expectation of success **must be found in the prior art and not based on the Applicant's disclosure**.  *See In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991) (emphasis added).

As mentioned, the subject invention generally relates to a system that automates security in an industrial control environment by automatically creating security profiles for industrial automation devices in the environment and enforcing these profiles with respect to accessing entities.  Such profiles may define different levels of access for various entities.  To this end, independent claim 20 recites *a server that manages a* *network interface between networked industrial automation devices* and *other devices attempting access to the networked industrial automation devices; and a security management module associated with the network interface that enforces an enterprise wide policy and that **manages security threats directed to the networked industrial automation devices**.*  Flowers, *et al.* and Abraham, *et al.*, when taken alone or in combination, fail to disclose, teach, or suggest such claimed aspects.

Flowers, *et al.* generally relates to allowing a vulnerability detection system and an intrusion detection system, for conventional networked computer environments, to interoperate with each other such that the intrusion detection system can utilize information received from the vulnerability detection system to choose areas for monitoring. (*See* col. 1, line 18 to col. 2, line 60). Another aspect of the cited reference is to ease the use and configuration of such components for a systems engineer. Accordingly, the vulnerability detection portion of the system is able to interrogate other systems on the network to determine potential weaknesses within the system. The data gathered from this component is stored with a way to cure the weakness, and the intrusion detection system may utilize this information for its subsequent operations. However, Flowers, *et al.* is silent regarding a system operable with ***industrial automation devices***.

For this reason, Flowers, *et al.* does not disclose a server that manages a network interface between networked industrial automation devices or managing security threats to such devices. Examiner does not properly reject the former, but provides Abraham, *et al.* to cure the latter. However, Abraham, *et al.* does not make up for the deficiencies of Flowers, *et al.* Specifically, Abraham, *et al.* does not disclose a system that manages security threats directed to the networked industrial automation devices; rather, as shown *supra*, Abraham, *et al.* merely discloses a system for regulating access to data that will be used in an industrial process at some time in the future. Moreover, independent claims 24 and 28 recite similar aspects with respect to securing industrial automation devices.

For at least the foregoing reasons, Flowers, *et al.* and Abraham, *et al.*, when taken alone or in combination, fail to disclose, teach, or suggest each element as recited in independent claims 20, 24, and 28. Therefore, rejection of these claims, as well as claims 21-23 and 25-27 which depend therefrom, should be withdrawn.

### III.    Rejection of Claim 8 Under 35 U.S.C. §103(a)

Claim 8 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Abraham, *et al.* This rejection should be withdrawn for at least the following reason. Abraham, *et al.* has been shown insufficient in regard to rejection of claim 1 under 35 U.S.C. §102(b), *supra*. Since claim 8 depends from claim 1 which has been shown as

valid, Abraham, *et al.* is insufficient to reject claim 8 under 35 U.S.C. §103(a), and accordingly, this rejection should be withdrawn.

## CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USA].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

 /Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731